

#2
11-20-02
gm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 30003052-2

J1050 U.S. PTO
10/075380
02/15/02

Applicant: Richard BROWN et al.
Title: IMPROVEMENTS IN AND RELATING TO DIGITAL
CERTIFICATES
Appl. No.: Unassigned
Filing Date: 02/15/2002
Examiner: Unassigned
Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

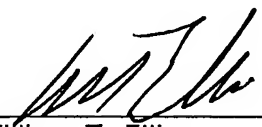
In support of this claim, filed herewith is a certified copy of said original foreign application:

Great Britain Application No. 0103969.2 filed February 17, 2001.

Respectfully submitted,

February 15 2002
Date

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400



William T. Ellis
Registration No. 26,874

This Page Blank (uspto)



INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ



the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

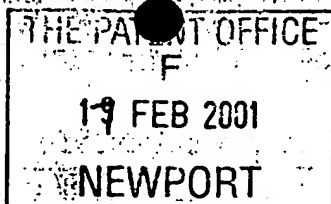
In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 9 April 2001

**CERTIFIED COPY OF
PRIORITY DOCUMENT**



19FEB01 E607054-1 D01463
P01/7700 0.00-0103969.2

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference 30003052 GB

2. Patent application number
(The Patent Office will fill in this part)

0103969.2

17 FEB 2001

3. Full name, address and postcode of the or of each applicant (underline all surnames)

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number (if you know it) 496588004

Delaware, USA

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention Improvements In and Relating To Digital Certificates

5. Name of your agent (if you have one)

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

Richard A. Lawrence
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

Patents ADP number (if you know it) 756308 3001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country Priority application number Date of filing
(if you know it) (day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

Yes

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note (d))

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document

Continuation sheets of this form

Description

11

Claim(s)

4

Abstract

1

Drawing(s)

2 + 2 SW

10. If you are also filing any of the following, state how many against each item.

Priority documents

-

Translations of priority documents

-

Statement of inventorship and right to grant of a patent (Patents Form 7/77)

1

Request for preliminary examination and search (Patents Form 9/77)

1

Request for substantive examination (Patents Form 10/77)

-

Any other documents
(please specify)

Fee Sheet

11. I/We request the grant of a patent on the basis of this application.

Signature

Richard A. Lawrence

Date

16/02/2001

12. Name and daytime telephone number of person to contact in the United Kingdom

Meg Joyce

Tel: 0117-312-9068

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- b) Write your answers in capital letters using black ink or you may type them.
- c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- e) Once you have filled in the form you must remember to sign and date it.
- f) For details of the fee and ways to pay please contact the Patent Office.

Improvements In and Relating to Digital Certificates

The present invention relates to digital certificates and to methods of communication.

5

A credential is a data structure provided to a bearer for a purpose, with some acknowledged way to verify the bearer's right to use the credential. A credential relates to an attribute, normally, but not necessarily, of the bearer. A credential is verified by a trusted source (sometimes referred to as the verifier). Often, there will be a chain of credentials and respective trusted sources until a verification is proffered by an organisation in which trust is implicit. Credentials are
10 incorporated in a digital certificate for verification.
15

A digital certificate generally comprises a file containing information, which file is transmitted to a recipient together with a digitally signed version thereof. The digitally signed version is a hash of the
20 file encrypted using a secret key (in a public key infrastructure). A hash is a one-way function that generates a substantially unique output from a file and is for all practical purposes irreversible. These concepts
25 are familiar to those skilled in the art.

Digital certificates are used in communication using distributed electronic networks, such as the internet, to transmit a credential, typically of the bearer. A known
30 digital certificate is the X.509 standard.

A certificate may contain one or more credential attributes.

A credential attribute in a certificate can be almost anything. Typical examples relevant to the present invention may be a credit rating, an access authorisation
5 (for physical or electronic access), a verification of identity etc.

Each attribute has at least one attribute property, such as a value (e.g. a numeric or alphanumeric) or something
10 more complex such as an indication of trust.

Generally, known digital certificates are valid for a fixed period of time (e.g. 1 year), during which time they will be used as a means of authentication and for gaining
15 authorised access to services etc. This is referred to as the valid period. Such digital certificates can, however, be revoked at any time by the verifier (terminating the valid period), thus placing a burden on the certificate recipient to check revocation lists or to use online
20 certificate status protocol services. These certificates are generally valid or not valid; there is no middle ground even though the degree of trust the trusted source has in the credential attribute may, in fact, vary over time (or some other variable) or if there is a wish to
25 vary the credential attribute value.

A certificate may still be in a valid period even if a credential attribute within it is not.

30 By way of example, a certificate may specify an individual's credit limit as a credential attribute. While this may be correct at the time of generation of the certificate, within the typical one year limit of the

certificate, the verifier may not wish to attest to the same credit limit for the full period.

In another example a credential attribute may allow entry
5 to a building which a certificate provider may wish to restrict to certain days.

Preferred embodiments of the present invention aim to address the problems referred to above.

10

According to the present invention in a first aspect, there is provided a digital certificate, the certificate comprising a credential attribute function associated with a credential attribute property, in which the credential
15 attribute function determines the value of the credential attribute property.

Suitably, there is provided a digital certificate comprising a credential attribute and at least one
20 credential attribute property, the certificate having a valid period, and a credential attribute function associated with the at least one credential attribute property, which function determines the value of the credential attribute property within the valid period.

25

The "property" value need not be a numerical value, though generally it will be so. Numerical property values may relate to a numerical attribute, e.g. a credit rating, or be a numerical representation of a confidence level in a
30 particular credential attribute e.g. that of identity of the bearer. Typically, for a confidence level, the value will be between a zero trust number (say '0' or '-1') and

a full trust number (say '1') attributing a high confidence level to the credential.

Other values may be alphanumeric e.g. "YES"/"NO" outputs
5 or relate to preset word based indications such as "HIGH TRUST", "MEDIUM TRUST" or "LOW TRUST".

By having the attribute function within the certificate it can be trusted by the recipient as a verified
10 determination of the credential attribute property value.

Suitably, the credential attribute function varies the credential attribute property value as a function of time. The attribute function may be monotonically decreasing
15 over time.

Suitably, the credential attribute function is configured to determine the credential attribute property value automatically. Suitably, the credential attribute
20 function is embedded within the certificate as an executable file. Suitably, execution of the executable file determines the credential attribute property value. Suitably, the executable file is a platform portable code, such as Java Script or HTML.

25

Suitably, the credential attribute property comprises a value operated on by the credential attribute function to determine a credential attribute property value.

30 Suitably, the credential attribute function uses data obtained from outside the certificate to determine the credential attribute property value. Suitably, the obtained data is obtained from a user by the input of data

in response to a query generated by the function. Suitably, the obtained data is obtained from a digital data store. Suitably, the digital data store is a web site.

5

Suitably, there is a plurality of credential attributes in the certificate. Suitably, there is a plurality of credential attribute properties in the certificate. Suitably, a plurality of the credential attribute
10 properties have respective attribute functions. Suitably, each credential attribute property has a respective attribute function.

Suitably, the certificate has a valid period and the
15 credential attribute function determines the value of the credential attribute property within the valid period.

According to the present invention in a second aspect, there is provided a method of communication, which method
20 comprises the steps of communicating from a sender to a recipient a digital certificate according to the first aspect of the invention.

Suitably, the recipient inspects the certificate and the
25 credential attribute property value is determined according to the credential attribute function.

Suitably, the communication at least in part is via a distributed electronic network.

30

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a schematic representation of a digital certificate according to a first embodiment of the present invention.

5

Figure 2 is a schematic representation of a distributed electronic network over which the present invention may be used.

10 Figure 3 is a schematic representation of a digital certificate according to a second embodiment of the present invention.

Referring to Figure 1 of the drawings that follow there is shown, schematically, a digital certificate 2 according to the X.509 standard, the certificate 2 containing a credential attribute 4, having a credential attribute property 5 and an associated credential attribute function 6. The certificate 2 is digitally signed (a hash created, which hash is encrypted using a verifier's secret key) as indicated at 8.

In the certificate 2, it will be appreciated that many of the fields present in an X.509 certificate are not represented. These may include fields containing data to allow a credential attribute property value to be determined or evaluated according to the credential attribute function 6. For instance, these fields may include a credential start date.

30

The credential attribute function 6 is embedded in the certificate 2 as an executable file of platform portable code such as JavaScript or HTML.

The certificate 2 is communicated via a distributed electronic network, such as the internet, as shown schematically in Figure 2 of the drawings that follow, in which a sender 14 communicates with a recipient 16 via the internet, indicated schematically at 18. An external data source from which data can be obtained is indicated schematically at 20. Communication can be via other distributed electronic networks, such as Wide Area Networks (WANs) or Local Area Networks (LANs). Embodiments of the present invention can also be implemented in other, less preferred, ways, for instance by storing a certificate on a digital storage device (e.g. a floppy disk) and sending this to the recipient 16.

Upon receipt of the digital certificate 2, the recipient 16 inspects the digital signature 8 to verify the certificate 2. Having done so, the recipient 16 executes the credential attribute function 6 which operates on the credential attribute property 5 (indicated schematically at 10) to determine a credential attribute value 12. The determined credential attribute value 12 becomes the credential attribute value 12 for the recipient 16.

By way of example, the credential attribute property may be a credit rating for a bearer of the certificate. The credit limit in the credential attribute property may be, say, £10,000. The function 6, in this case, is a modifier of the credential attribute value 12. Pursuing the example of the credit rating, the function 6 may be to reduce the rating by 10% of the original rating for each month. Applying the function 6 to the attribute value 4 above, the function obtains date information and in the

second month the credential attribute value 4 is determined as £9,000 and so on. Date information may be obtained from the recipient computer or, for more security, from a trusted source, preferably a trusted source web site. These are digital data sources.

In another example the credential attribute property 4 may be an access authorisation for a building to which the provider of the certificate 2 only wishes to allow the certificate bearer access on specified times, say week days only. The credential attribute property 4 would have a value of "PERMIT ACCESS" in this case. The function 6 is, therefore, encoded to determine the day of the week (for instance from a computer on which the certificate 2 is being verified, or from a remote web-site) and generate a modified credential attribute property value which is "DO NOT PERMIT ACCESS" at week ends. It will be appreciated from this that the credential attribute property 4 will not always be modified by function 6.

Alternatively, the credential attribute property 4 may not have an original value in the certificate. Instead, it may solely be generated by a credential attribute function which (generally) obtains data externally of the certificate.

Referring to Figure 3 of the drawings that follow, there is shown a schematic representation of a digital certificate 32 corresponding to digital certificate 2 of Figure 1, except that in digital certificate 32 there is a plurality of credential attributes 34A-34N with associated credential attribute properties 36A-36M and corresponding

credential attribute functions 38A-38P. The certificate 32 is signed, as indicated at 40.

In this example credential attribute 34A is a credit
5 limit, having properties of a value 36A and an indication
of trustworthiness 36B. Other properties 36C etc may be
included. Credential attribute 34N is an identity having
a value 36L and an indication of trustworthiness 36M.

- 10 Each function 38A-38P is capable of modifying a respective
credential attribute property 36A-36M to determine a
respective credential attribute property value 42A-42M
obtaining external data as required as indicated at 44A-G.
- 15 There may be a one-to-one correlation between each
credential attribute property 34A-34N and its
corresponding function 36A-36N, though this need not be
the case. For instance, one or more, but not necessarily
all, of the credential attribute properties 34A-34N need
20 have a credential attribute function 36 for generation
thereof. Further, a given credential attribute function
38A-38P may be used for a plurality of credential
attribute properties 34A-34N, in which case there may be
fewer functions 36 than credential attribute properties
25 34.

Thus the certificate may provide the recipient with
credential attribute property values relevant to a
plurality of attributes therein.

30

The function can seek information from elsewhere on which
to base its generation of the credential attribute
property value. For instance, the function 6 can access

local time data or extract data from a web-site as required, as described above. Alternatively, in a less preferred option, data can be sought from the recipient of the certificate in response to an enquiry generated by the
5 credential attribute function. This option is less preferred as it makes the certificate less self-contained.

The function 6 may obtain all its data for producing the credential attribute property value from external of the
10 certificate.

In less preferred embodiments the function 6 can be a non-automated modifier of a credential attribute property. For instance, the function 6 could be a written statement
15 that an attribute property is to decrease by a certain amount per time unit. However, it is preferred that the function 6 be automated so that a modified credential attribute property is generated automatically.

20 The digital certificate may, optionally, be encrypted.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and
25 which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification
30 (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination,

except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including
5 any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series
10 of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extend to any novel one, or any novel combination, of the features disclosed
15 in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Claims

1. A digital certificate, the certificate comprising a credential attribute function associated with a credential attribute property, in which the credential attribute function determines the value of the credential attribute property.
5
2. A digital certificate according to claim 1, in which there is provided a digital certificate comprising a credential attribute and at least one credential attribute property, the certificate having a valid period, and a credential attribute function associated with the at least one credential attribute property, which function determines the value of the credential attribute property within the valid period.
10
15
3. A digital certificate according to claim 1 or claim 2, in which the credential attribute function varies the credential attribute property value as a function of time.
20
4. A digital certificate according to claim 3, in which the credential attribute function is monotonically decreasing over time.
25
5. A digital certificate according to any preceding claim, in which the credential attribute function is configured to determine the credential attribute property value automatically.
30

6. A digital certificate according to any preceding claim, in which the credential attribute function is embedded within the certificate as an executable file.
- 5 7. A digital certificate according to claim 6, in which execution of the executable file determines the credential attribute property value.
- 10 8. A digital certificate according to claim 6 or claim 7, in which the executable file is a platform portable code, such as Java Script or HTML.
- 15 9. A digital certificate according to any preceding claim, in which the credential attribute property comprises a value operated on by the credential attribute function to determine a credential attribute property value.
- 20 10. A digital certificate according to any preceding claim, in which the credential attribute function uses data obtained from outside the certificate to determine the credential attribute property value.
- 25 11. A digital certificate according to claim 10, in which the obtained data is obtained from a user by the input of data in response to a query generated by the function.
- 30 12. A digital certificate according to claim 10, in which the obtained data is obtained from a digital data store.

13. A digital certificate according to claim 12, in which the digital data store is a web site.
14. A digital certificate according to any preceding
5 claim, in which there is a plurality of credential attributes in the certificate.
15. A digital certificate according to any preceding
10 claim, in which there is a plurality of credential attribute properties in the certificate.
16. A digital certificate according to claim 15, in which a plurality of the credential attribute properties have respective attribute functions.
15
17. A digital certificate according to claim 16, in which each credential attribute property has a respective attribute function.
- 20 18. A digital certificate according to any preceding claims, in which the certificate has a valid period and the credential attribute function determines the value of the credential attribute property within the valid period.
25
19. A method of communication, which method comprises the steps of communicating from a sender to a recipient a digital certificate according to any preceding claim.
- 30 20. A method of communication according to claim 19, in which the recipient inspects the certificate and the credential attribute property value is determined according to the credential attribute function.

21. A method of communication according to any preceding claim, in which the communication at least in part is via a distributed electronic network.

5

22. A digital certificate substantially as described herein, with reference to and as shown in the accompanying Figures 1 or 3.

10 23. A method of communication substantially as described herein, with reference to the accompanying Figures 1 and 2 or 2 and 3.

ABSTRACT

Improvements In and Relating to Digital Certificates

5 The present invention provides a digital certificate (2,
32), the certificate comprising a credential attribute
function (6, 38) associated with a credential attribute
property (5, 36), in which the credential attribute
function determines the value (12, 44) of the credential
10 attribute property. A corresponding method is also
disclosed.

15

Figure 1

FIGURE 1

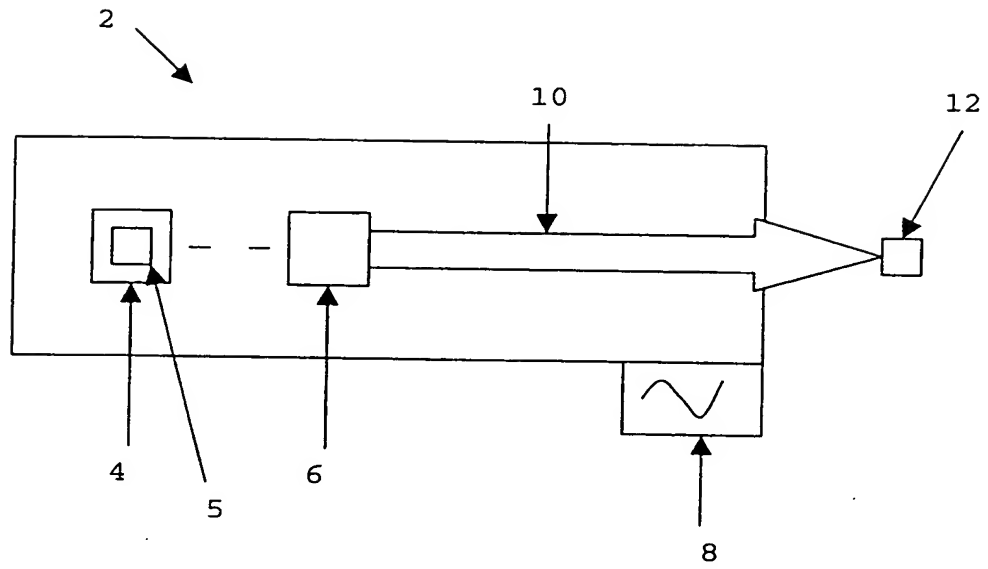
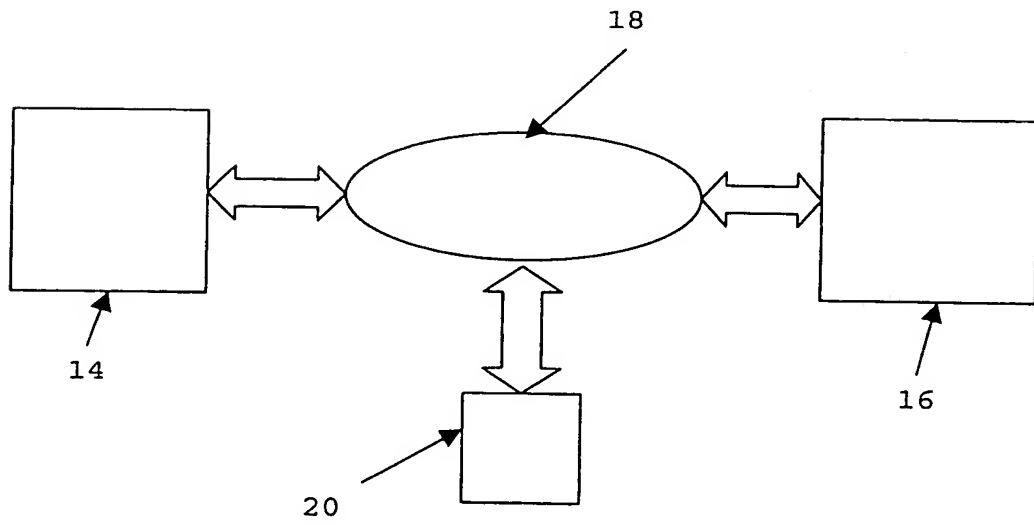
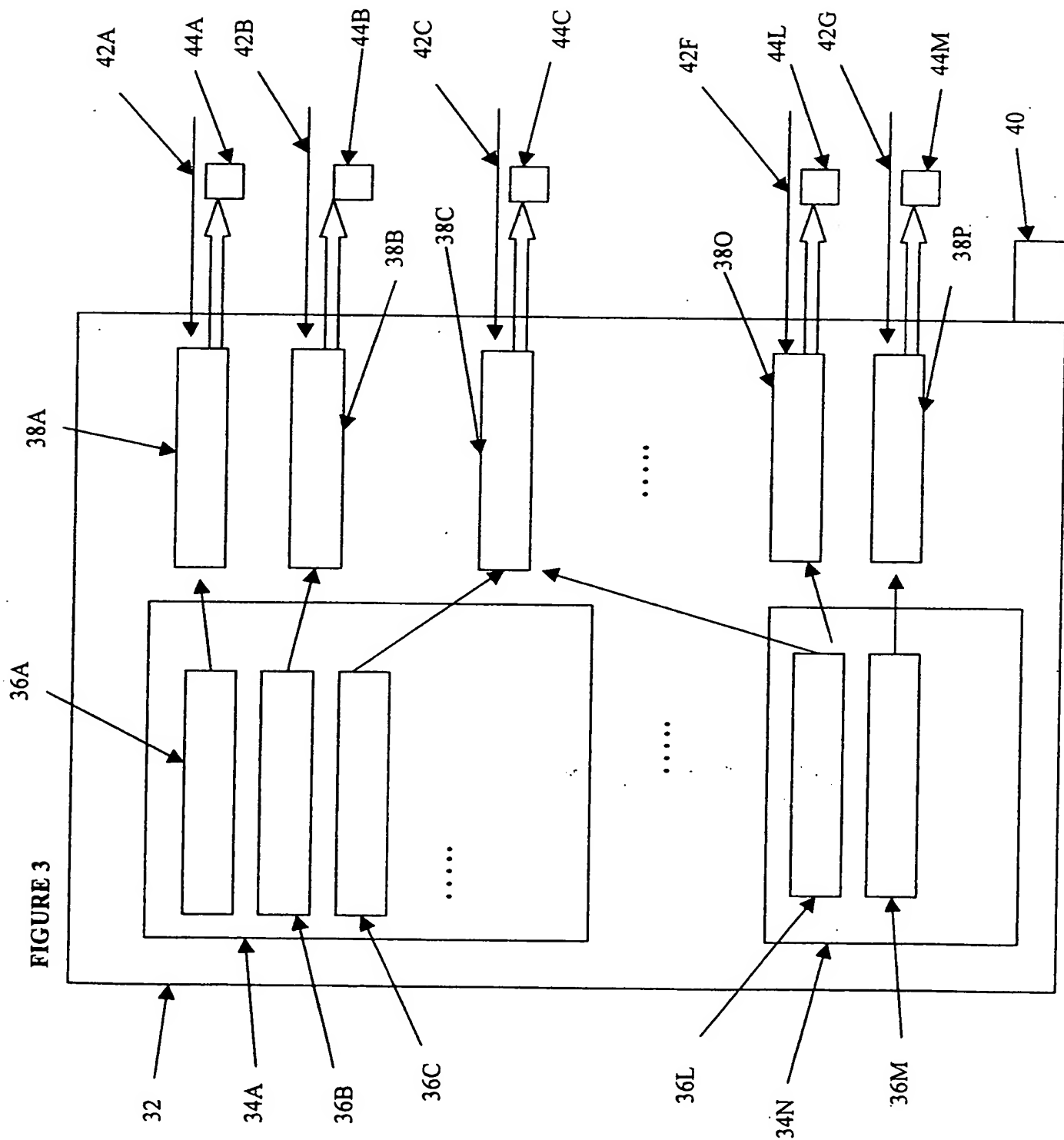


FIGURE 2



This Page Blank (uspto)

FIGURE 3



This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)